Device and method for protecting sensitive data and franking machine using them

The present invention relates to a device and a method for protecting sensitive data and to a franking machine using them.

It applies in particular to franking machines with a program running in a multitask environment and more generally to the protection of sensitive data, for example data representing amounts of money, or of sensitive tasks manipulating the sensitive data.

In a multitask environment, each task can invoke each routine, regardless of the security necessary for said routine. In a franking machine, some tasks manipulate quantities representing amounts of money. In particular, the phases of operating or recharging a franking machine use the routines that manipulate amounts of money.

The correct execution of each of these tasks must be guaranteed. By "correct execution" is meant the fact that a task executes in the normal context of operation of the machine. In other words, the invention seeks to prevent that sensitive data be degraded or modified inopportunely.

To this end, the present invention aims to have at least one routine operating on sensitive data verify the identity of tasks that invoke it.

Accordingly, if an unauthorized task attempts to invoke said routine, the latter can limit its execution and therefore prevent harm to the sensitive data concerned.

According to a first aspect, the present invention provides a method of protecting sensitive data against use of a routine operating on said data, characterized in that it includes an operation of verifying the identity of each software task calling said routine, which operation is implemented by said routine.

Thanks to these features, if an unauthorized task is used to access said routine which uses sensitive data, on verifying its identity, that routine detects that it is not authorized and it prevents access to the sensitive data concerned.

In the case of a franking machine, for example, the routines concerned include the routine for incrementing the counter for the franking amount consumed and decrementing the counter for the remaining available franking amount and the routine for incrementing the counter for the number of franking operations effected.

In accordance with particular features, said verification operation includes an operation of reading an identifier of said task and an operation of comparing said identifier with predetermined identifiers.

Thanks to these features, all the tasks authorized to use the routine in question are identified in a particular list, which facilitates programming the routine and updating the programming.

According to other particular features, each routine operating on said data implements said verification operation.

Thanks to these features, whichever routine attempts to access the sensitive data, the protection offered by the present invention is assured by said routine.

According to a second aspect, the present invention provides a device for protecting sensitive data against use of a routine operating on said data, characterized in that it includes a verification system adapted to verify the identity of each software task calling said routine, said verification system being implemented by said routine.

The invention also provides a franking machine characterized in that it includes a device as succinctly

described above.

The invention is also directed to:

- a system for storing information readable by a computer or a microprocessor storing instructions of a computer program, characterized in that it enables to implement the method according to the invention as succinctly described hereinabove, and

- a partly or completely removable system for storing information readable by a computer or a microprocessor storing instructions of a computer program, characterized in that it enables to implement the method according to the invention as succinctly described hereinabove.

The above device, the above franking machine and the above storage system having the same particular features and the same advantages as the method succinctly described hereinabove, the advantages are not described again here.

Other advantages, objects and features will emerge from the following description, which is given with reference to the accompanying drawings, in which:

- figures 1A and 1B are respectively a plan view and an elevation view of a franking machine using the device and the method of protecting data which are the subject-matter of the invention,

- figure 2 represents schematically an electronic circuit incorporated in the franking machine shown in figures 1A and 1B, and

- figure 3 shows an operation algorithm of the electronic circuit shown in figure 2.

The franking machine 1 shown in the drawings (figures 1A and 1B) includes a device for printing a franking mark and an optional destination address on a flat object such as a letter 2.

In order to print the franking mark in the

standardized place provided for this purpose, the letter 2 must be passed through a corridor 5 included in the machine 1, said corridor being delimited by members fastened to the frame, respectively a sliding support 6 which forms the ceiling of the corridor 5, a table 7 which forms its floor, and a ramp which forms a lateral limit thereof, the corridor being open at the end opposite the ramp.

In order to insert the letter 2 into the corridor 5, the letter is placed on the part of the table 7 which projects on the insertion side (the side seen on the left in figure 1B), after which the letter is inserted into the corridor 5, as shown in figures 1A and 1B, until it is driven by the means provided for this purpose in the machine 1. The printing of the franking mark is performed automatically while the letter 2 is driven in the corridor 5, the franked letter being expelled from the machine at the other end of the corridor 5 (the end seen on the right in figure 1B).

For driving the letter 2, the machine 1 includes two rollers 9 and 10, each passing through an opening in the table 7, and respective pressure rollers 12 and 13 for the rollers 9 and 10, each passing through an opening in the support 6.

The rollers 9 and 10 are rotatably mounted with respect to the frame of the machine 1, through a suspension system 14 shown diagrammatically in figure 1B.

The pressure rollers 12 and 13 are rotatably mounted on the frame of the machine 1, without being suspended therefrom. An electric motor, not shown, is used to drive synchronous rotation of the pressure rollers 12 and 13, for example through a belt (not shown) running around three pulleys respectively carried by the motor, the pressure roller 12 and the pressure roller 13.

Because the suspension system 14 urges the rollers 9 and 10 toward the support 6, and therefore toward the

pressure rollers 12 and 13, the rollers 9 and 10 are driven by friction against the pressure rollers 12 and 13, either directly or through an object passing through the machine 1, such as the letter 2.

When the letter 2 is inserted into the corridor 5 in the manner shown in figure 1B, it eventually encounters the roller 9 and then the pressure roller 12, which drives it in the direction indicated in figure 1B by the horizontal arrow oriented from left to right. At the same time, the roller 9 is lowered whereas the letter 2 is inserted between the rollers 9 and 12, so that the letter 2 moves forward in the machine 1 with its face 4 to be printed pressed against and sliding along the surface 17 of the sliding support 6.

For printing the franking mark in its corresponding standardized place and/or the destination address in its corresponding standardized place, the machine 1 includes a printing system 19, shown quite diagrammatically in figures 1A and 1B.

Generally speaking, the printing system 19 applies the franking mark while the letter 2 or the object to be franked is travelling through the machine 1 with its face to be printed pressed against the surface 17 of the sliding support 6, the printing system 19 being located between the pressure rollers 12 and 13.

In the example shown, the printing system 19 is mounted directly on the frame of the machine and is therefore fixed relative to the sliding support 6.

In order for the printing system 19 to be controlled synchronously with forward movement of the object in the machine, there is provided a detector (referenced 110 in figure 2) of the presence of the object which triggers a printing process running automatically.

To be more precise, there is a first presence detector that causes the motor (not shown) to be started

when an object begins to be inserted into the machine 1, and a second presence detector (not shown) that triggers the printing process when the object has reached a predetermined location.

Figure 2 shows an electronic circuit for controlling the device has shown in figures 1A and 1B. The circuit 100 is illustrated in the form of a block diagram. It includes, connected together by an address and data bus 102:

- a central processing unit 106,
- a random access memory (RAM) 104,
- a read-only memory (ROM) 105,
- an input/output port 103 for receiving:
  - the weight of the postal object to be franked, and
  - detection of the postal object by each of the detectors (not shown in the figures),

  and for transmitting:
  - motor control signals,

  and, independently of the bus 102:
- stepper motors 109;
- presence detectors 110;
- a display screen 108 connected to the input/output port 103,
- scales 112 connected to the input/output port 103 and supplying bytes representing the weight of a postal object,
- a keypad 101 connected to the input/output port 103 and supplying bytes representing successively pressed keys of the keypad, and
- a printing controller 120 controlling the operation of the printing sytem 19.

Each of the components shown in figure 2 is well known to the person skilled in the art of franking machines having a microprocessor circuit and, more generally, information processing systems. Those components are

therefore not described here.

The random-access memory 104 stores data, variables and intermediate processing results in memory registers which, in the remainder of the description, carry the same name as the data whose value they store. The random-access memory 104 includes notably registers storing information representing the weight of the postal object to be franked, the format of the postal object currently being processed, the number of postal objects in the batch currently being processed, up-counter and down-counter values that correspond to franking amounts already applied and remaining to be applied before recharging the machine. The latter registers operate according to techniques that are known in the field of franking machines (during each franking operation, when the down-counter amount is greater than the amount of the franking mark to be applied, it is decremented by the amount of that mark and the up-counter is incremented by the same amount).

The read-only memory 105 is adapted to store the operating program of the central processing unit 106 in a register labeled *"program1"*, and the data needed for operation of that program as well as a correspondence table relating weights and franking amounts.

The read-only memory 105 also stores in a register labeled *"identifier_list"* a list of identifiers of software tasks authorized to access the routines that use sensitive data (e.g. franking amounts).

The memory 105 referred to as a "read-only memory" is in fact a rewriteable memory that is not erased when the device is turned off. It can be rewritten only by authorized personnel using secure procedures, so that for the everyday user it is just like a read-only memory.

The central processing unit 106 is adapted to use the program stored in read-only memory 105. An operating algorithm of that program is shown in figure 3.

The software (program) of the franking machine is a multitask software, which implies allocation by the processor of a memory space (stack) associated with each task. This memory space is included in the random access memory 104.

During an operation 301:

- the electronic card 10 is initialized by the central processing unit 106, using known techniques, and
- the central processing unit 106 assigns an identifier (e.g. a number) to each task of the application.

During an operation 302, the central unit 106 runs a program portion that does not necessitate any call to a routine using sensitive data.

During an operation 303, the central unit 106 implements a task that calls one of the routines that use sensitive data.

During an operation 304, the routine 400 in question (shown in dashed line) reads the identifier of the task currently being run by calling a so-called "system" routine of a known type, intended for that read operation.

Then, during a test 305, the routine 400 compares the identifier of the task to the content of the list of identifiers stored in the read-only memory 105 and determines whether that task identifier is in the list.

When the result of the test 305 is positive, the task is authorized to access the routine and the use of sensitive data is executed during an operation 306. The central unit 106 then returns to the operation represented by the reference 302.

When the result of the test 305 is negative, the task is not authorized to access the routine. The operation of the central unit 106 is then stopped, and an alarm is tripped (operation 307), until the franking machine is powered down (operation 308).

Thus, the method of protecting sensitive data

against use of a routine operating on said data, provided by the present invention, includes an operation 400 of verifying the identity of each software task calling said routine, which operation is implemented by said routine.

Thus, thanks to the organization of the task 400, and in particular thanks to the monitoring of the identity of the tasks that call it, the modification of the sensitive data by means of this routine is impossible.

As a variant, the routines 400 (i.e. the routines that verify the identity of the task calling them before accessing sensitive data) include not only the routines that access the franking amount counters but also routines operating on statistical data or operating parameters of the franking machine.

In the embodiment described and shown, said verification operation 400 includes an operation 304 of reading an identifier of said task and an operation 305 of comparing said identifier with predetermined identifiers.

In the embodiment described and shown, each routine operating on sensitive data implements said verification operation 400.

The device for protecting sensitive data against use of a routine operating on said data is characterized in that it includes as a verification system the central unit 106, associated with memories 104 and 105, for verifying the identity of each software task calling said routine, this verification system being implemented by said routine.